COMMUNICATIONS EQUIPMENT SOFTWARE NOTE 6
(for Electronics Technicians)
Maintenance, Logistics, and Acquisition Division
W/OPS12: GSS

SUBJECT:	CRS Build 10.0 and VIP Build 3.1 Software Installation Procedures
PURPOSE:	This document contains the procedures for installing the Console Replacement System (CRS) Build.10.0 software and the Voice Improvement Processor (VIP) Build 3.1 software. The tasks necessary for installing the CRS and VIP software are included in attachment A.
SITES AFFECTED:	All CRS sites
EQUIPMENT AFFECTED:	CRS (B440)
PARTS REQUIRED:	W/OPS12 will issue the following parts to each site under the appllicable approved site-specific Request for Change: (1) CRS Build 10.0 Installation CD (6) VIP Installation CDs labeled VIP OS Restore 1 through 6
PARTS SUPPLIED BY THE SITE:	The site will provide: (4-6) Blank diskettes for saving VIP Version 3.0.1 pre-processor substitution and local dictionaries. (1) Blank DOS-formatted diskette that will contain the Secure Shell (SSH) keys. (This note provides instructions for creating this diskette.)
TOOLS AND TEST EQUIPMENT REQUIRED:	None.
TIME REQUIRED:	6.0 hours.
EFFECT ON OTHER INSTRUCTIONS:	None.
AUTHORIZATION:	The authority for his modification is Request for Change AC189.
VERIFICATION STATEMENT:	This procedure was tested and verified at National Weather Service Headquarters (WSH), Silver Spring, MD (SLVM2).
GENERAL:	This procedure contains instructions for replacing the CRS and VIP software.
TECHNICAL ASSISTANCE:	For questions or problems pertaining to this software note, please contact Nancy Helderman at (301) 713.0191 ext. 139 or Joel Nathan at (301) 713-0191 ext. 119.

PROCEDURE:	Attachment **A** provides procedures for implementing this modification. Attachment **B** provides a completed Engineering Management Reporting System (EMRS) report sample.
REPORTING INSTRUCTIONS:	Report the completed modification using the EMRS according to the instructions in the NWS Instruction 30-2104, Maintenance Documentation, Part 4 and Appendix G. Include the following information in the report. a. Equipment Code: **CRSSA** b. Serial Number: **001** c. Mod Number: **S6** A sample EMRS report is provided as attachment **B**.

Signature Not Verified

Mark S. Paese

Digitally signed by Mark S. Paese
DN: cn=Mark S. Paese, o=DOC/NOAA/NWS, c=US
Date: 2004.09.20 16:01:39 -04'00'

Mark S. Paese
Director, Maintenance, Logistics, and Acquisition Division

Attachment **A** - Installation Procedures
Attachment **B** - Sample EMRS Report

ATTACHMENT A
Installation Procedures

Overview

NOTE:	No changes have been made to the current CRS Build 9.0.1 operational database. Therefore, you will be able to use your old database with the new Build 10.0 CRS software. After installing the new software, you will be able to restart the CRS application software and run it with the old database. No changes to the database are necessary.

This software note provides instructions for performing the CRS and VIP software upgrades. The installation procedure consists of ten parts:

1. Pre-Installation Procedures

2. Backup of VIP Pre-Processor Substitution and Local Dictionaries (requires 4 - 6 blank diskettes)

3. Termination of VIP Build 3.0.1 Application Software and Shutdown of Operating System

4. Installation and Startup of VIP Operating System and Build 3.1 Application Software

5. Recovery of VIP Pre-Processor Substitution and Local Dictionaries

6. Termination of the CRS Build 9.0.1 Application Software

7. Installation and Verification of CRS Build 10.0 Application Software and Modification to Man Machine Interface (MMI) To Remove Unwanted Messages

8. Changing of MP, FEP, and LAN Server Passwords

9. Installation of SSH Keys

10. CRS and VIP Application Startup and Verification

The following will be needed before proceeding with the installation procedures:

1	CRS Build 10.0 Installation CD (provided by W/OPS12 in delivery package)
6	VIP Installation CDs labeled “VIP OS Restore 1 through 6” (provided by W/OPS23 in delivery package)
2 - 6	Blank diskettes for saving “VIP Version 3.0.1” dictionaries.
1	Blank DOS-formatted diskettes labeled “SSH Keys.”

PART 1 - PRE-INSTALLATION PROCEDURES

1.1 Scheduling CRS Downtime

1. As a conservative estimate, schedule 6 hours to perform the software note (2 hours for VIP installation, 1 hour for CRS installation, and 15 minutes for SSH key installation). This is a conservative estimate. The actual installation time may be less, or it may be more if you encounter problems.
2. Before proceeding with the modification, read the entire procedure.
3. Notify the public that CRS (NOAA Weather Radio) will be down during this scheduled time for maintenance.
4. If you are currently logged into the *CRS Main GUI*, skip to step 7. Otherwise, the *CRS Security Warning* message window displays.
5. Click **Acknowledge**. The *CRS Login* screen displays.
6. Log in to the *CRS Main GUI* menu as **admin**. (The *Security Warning* window redisplays after 30 seconds if a user ID and password are not entered.)
7. From the *CRS Main GUI*, click **Maintenance** and click **UNIX Shell**.
8. Enter the following command at the UNIX prompt:

   `ping -s 5MP`

   Press **<Enter>**. Every second a message displays that 64 bytes have been received from 5MP. After 1 minute, terminate the test by pressing the **<Del>** key. A message displays how many data packets were received and transmitted and the percentage of packet loss. If the number of packets received does not match the number transmitted and/or the percentage of packet loss is not zero (0), stop this procedure, and identify and correct the source of the data loss.
9. Repeat step 8 for all remaining FEPs and 4BKUP.
10. Enter the following command at the UNIX prompt to close the *UNIX Shell*:

    `exit`

    Press **<Enter>**.

PART 2 - BACKUP OF VIP PRE-PROCESSOR SUBSTITUTION AND LOCAL DICTIONARIES (requires 4 - 6 blank diskettes)

NOTE: 1. The dictionaries that are saved to diskette in this section will be restored in Part 5 after the new disk image has been installed. All sites will back up and restore the female (Donna) and male (Tom) dictionaries. Only sites with the Spanish license will back up and restore the Spanish (Javier) dictionaries.

2.1 Backup of Substitution Dictionaries

1. Place a blank formatted diskette in the VIP drive. From the main *VIP* menu, click **Pre-Processor**. This will display the *Pre-Processor "Substitution Dictionary" Manager*.
2. Click **Options**, which displays a *pull-down* menu. From the pull-down menu, click **English Male Substitution Dictionary <Tom>**.
3. Click **Options**, which displays a *pull-down* menu. From the pull-down menu, click **Save Current Substitution Dictionary To Floppy Disk**.

NOTE: 2. In the event of a floppy drive error, the operator might have to "unmount" the floppy drive. To perform this, bring up a UNIX shell, type **`unmount/mnt/floppy/`**, then type **`exit`** to return to the GUI server.

4. A dialog box is displayed that asks:

   Save the "Tom Substitution" dictionary to floppy disk?

   Click **Yes**.

5. If the transfer of the dictionary is successful, a dialog box will display the following message:

   File Transfer Successful! File saved on floppy as: "tom-sub.dic".

   Click **OK**.

6. Remove the **tom-sub.dic** diskette from the drive, label it as "**tom-sub.dic**," and store it in a safe place. Use this diskette whenever it is necessary to restore the English Male Substitution Dictionary. Please note that the operator has no choice in the name of the backup file; it will always be *tom-sub.dic*.
7. Place a blank formatted diskette in the drive. Click **Options**, which displays a *pull-down* menu. From the pull-down menu, click **English Female Substitution Dictionary <Donna>**.
8. Click **Options**, which displays a *pull-down* menu. From the pull-down menu, click **Save Current Substitution Dictionary To Floppy Disk**.

9. A dialog box is displayed that asks:

   Save the "Donna Substitution" dictionary to floppy disk?

   Click **Yes**.

10. If the transfer of the dictionary is successful, a dialog box will display the following message:

    File Transfer Successful! File saved on floppy as: "mara-sub.dic".

    Click **OK**.

11. Remove the **mara-sub.dic** diskette from the drive, label it as "**mara-sub.dic**," and store it in a safe place. Use this diskette whenever it is necessary to restore the English Female Substitution Dictionary. Please note that the operator has no choice in the name of the backup file; it will always be *mara-sub.dic*. If you do not have a Spanish license, skip to step 17.

12. Place a blank formatted diskette in the drive. Click **Options**, which displays a *pull-down* menu. From the pull-down menu, click **Spanish Male Substitution Dictionary <Javier>**.

13. Click **Options**, which displays a *pull-down* menu. From the pull-down menu, click **Save Current Substitution Dictionary To Floppy Disk**.

14. A dialog box is displayed that asks:

    Save the "Javier Substitution" dictionary to floppy disk?

    Click **Yes**.

15. If the transfer of the dictionary is successful, a dialog box will display the following message:

    File Transfer Successful! File saved on floppy as: "javier-sub.dic".

    Click **OK**.

16. Remove the **javier-sub.dic** diskette from the drive, label it as "**javier-sub.dic**," and store it in a safe place. Use this diskette whenever it is necessary to restore the Spanish Male Substitution Dictionary. Please note that the operator has no choice in the name of the backup file; it will always be *javier-sub.dic*.

17. Click the **black x** to exit from the *Pre-Processor "Substitution Dictionary" Manager* window.

2.2 Backup of Local Dictionaries

1. Place a blank formatted diskette in the VIP drive. From the main *VIP* menu, click **Dict Manager**. This will display the *Local Dictionary Manager*.

2. Click **Options**, which displays a *pull-down* menu. From the pull-down menu, click **English Male Dictionary <Tom>**.

3. Click **Options**, which displays a *pull-down* menu. From the pull-down menu, click **Save Current Dictionary To Floppy Disk**.
4. A dialog box is displayed that asks:

   Save the "Tom" dictionary to floppy disk?

   Click **Yes**.
5. If the transfer of the dictionary is successful, a dialog box will display the following message:

   File Transfer Successful! File saved on floppy as: "tom-root.dic".

   Click **OK**.
6. Remove the **tom-root.dic** diskette from the drive, label it as "**tom-root.dic**," and store it in a safe place. Use this diskette whenever it is necessary to restore the English Male Local Dictionary. Please note that the operator has no choice in the name of the backup file; it will always be *tom-root.dic*.
7. Place a blank formatted diskette in the drive. Click **Options**, which displays a *pull-down* menu. From the pull-down menu, click **English Female Dictionary <Donna>**.
8. Click **Options**, which displays a *pull-down* menu. From the pull-down menu, click **Save Current Dictionary To Floppy Disk**.
9. A dialog box is displayed that asks:

   Save the "Donna" dictionary to floppy disk?

   Click **Yes**.
10. If the transfer of the dictionary is successful, a dialog box will display the following message:

    File Transfer Successful! File saved on floppy as: "mara-root.dic".

    Click **OK**.
11. Remove the **mara-root.dic** diskette from the drive, label it as "**mara-root.dic**," and store it in a safe place. Use this diskette whenever it is necessary to restore the English Female Local Dictionary. Please note that the operator has no choice in the name of the backup file; it will always be *mara-root.dic*. If you do not have a Spanish license, skip to step 17.
12. Place a blank formatted diskette in the drive. Click **Options**, which displays a *pull-down* menu. From the pull-down menu, click **Spanish Male Dictionary <Javier>**.
13. Click **Options**, which displays a pull-down menu. From the pull-down menu, click **Save Current Dictionary To Floppy Disk**.

14. A dialog box is displayed that asks:

    Save the "Javier" dictionary to floppy disk?

    Click **Yes**.

15. If the transfer of the dictionary is successful, a dialog box will display the following message:

    File Transfer Successful! File saved on floppy as: "javier-root.dic".

    Click **OK**.

16. Remove the **javier-root.dic** diskette from the drive, label it as **javier-root.dic**, and store it in a safe place. Use this diskette whenever it is necessary to restore the Spanish Male Local Dictionary. Please note that the operator has no choice in the name of the backup file; it will always be *javier-root.dic*.

17. Click the **black x** to exit from the *Pre-Processor "Dictionary" Manager* window.

PART 3 - TERMINATION OF VIP BUILD 3.0.1 APPLICATION SOFTWARE AND SHUTDOWN OF OPERATING SYSTEM

3.1 Terminating the VIP Application

1. If the VIP application is running (the bottom of the main *VIP* menu displays *Running* on a green background), click **Stop**. If the VIP application is not running, skip to Section 3.2.

2. The bottom of the main *VIP* menu displays *Stopped* on a red background. The VIP application is stopped.

3.2 Shutting Down the VIP Operating System

1. Click **File** in the upper left area of the main *VIP* menu.

2. Click **System Shutdown**.

3. A dialog box displays asking if you want to shut down the VIP system. Click **Yes**. After a short time, the VIP computer shuts down.

PART 4 - INSTALLATION AND STARTUP OF VIP OPERATING SYSTEM AND BUILD 3.1 APPLICATION SOFTWARE

NOTE:
1. This procedure will take about 60 minutes to complete.
2. The hard drive image includes both the OS and the VIP Build 3.1 application. To restore the hard drive image, use the new VIP OS Restore CDs numbered 1 through 6. The old VIP OS Restore diskettes numbered 1 through 3 are no longer necessary. VIP OS Restore diskette #4 will remain as the bootable diskette to use if the VIP is unable to boot from the hard drive. Upon successful restoration of the hard drive image, store the new VIP OS Restore CDs in a safe place. Dispose of the old VIP OS Restore CDs and the old VIP OS Restore diskettes #1 through #3. Continue to store VIP OS Restore diskette #4 in a safe place.

4.1 Restoring the Hard Drive Image

1. Press the power button on the VIP computer to power up the computer. When the *F2 = Setup* message is displayed in the upper right corner of the screen, press **<F2>** to display the computer BIOS settings.
2. Insert the VIP **OS Restore #1 CD** into the CD drive and close it. Make sure there is no floppy in the A: drive.
3. Use the down arrow key to move the *blue selection bar* to **Boot Sequence** and press **<Enter>** to display the boot sequence.
4. The *IDE CD-ROM Device* must be **enabled** (indicated by a check mark to the left of the device name) and must be listed **before** the *Hard-Disk-Drive C:*. If both of these conditions are satisfied, press **<Esc>** twice and immediately skip to perform step 10 to prevent a prompt timeout (5-6 seconds). Otherwise, continue with the following steps.
5. Use the down arrow key to move the blue selection bar to *IDE CD-ROM Device*.
6. If the CD device is **enabled** (check mark), skip to step 7. Otherwise, change disabled (no check mark) to enabled (check mark) by pressing the space bar once.
7. If the *IDE CD-ROM Device* is listed **before** the *Hard-Disk-Drive C:*, skip to step 8. Otherwise, move the *IDE CD-ROM Device* to before the *Hard-Disk-Drive C:* by using the minus key.
8. Press **<Esc>** twice. A dialog box displays asking if the changes should be saved.
9. Select *Save Changes and Exit* and press **<Enter>**.
10. The VIP will start booting from the CD. A black text screen will appear.
11. Enter the following at the prompt:

    boot: **nuke noresize** and press **<Enter>**.

12. A black text screen appears with the following:

    Please specify an alternate tape device or hit [ENTER] to boot from CD/floppies.

13. Press **<Enter>** to boot from the CD.

14. The Mondo Rescue application will start. It displays a blue text screen with the message *WELCOME TO MONDO RESCUE* at the top. A *Caution* box displays with the warning:

    Be advised. I am about to ERASE your hard disks.

    It contains a countdown timer bar. Allow this countdown to expire and wipe clean and restore your existing VIP hard drive. The restore process will proceed through several screens of formatting and restoring data.

15. The first CD takes about 15 minutes to complete. During this time, the screen may become blank and black. To safely restore the screen, press the **right arrow** key.

16. You will be prompted with a prompt box titled *Alert* with the text phrase *Please insert CDR#2 and press Enter*. If the CD drive does not open automatically, open the CD drive with the eject button and replace CD #1 with the one titled *VIP OS Restore #2 CD*. Push the tray button and press **<Enter>**.

17. Repeat the previous step for CDs 3 through 6. CDs #2 through #5 CDs each take about 10 minutes to complete. CD #6 takes about 3 minutes. While the process is running, the screen will display messages *Restoring from archives* and *Reassembling large files,* each with a progress bar.

18. At the conclusion of the procedure, the following prompt in white text appears and the blue screen is pushed up by the black screen:

    *To reboot press **<Ctrl-Alt-Del>** together.*

    Remove the last CD, close the CD drawer, and press <**Ctrl-Alt-Del>**.

NOTE: 1. Sometimes the VIP will fail after the disk image has been restored. When the VIP starts booting, a “kernel panic” occurs. If this happens, a simple and fast procedure exists to correct the problem.

19. The Red Hat Linux 7.3 Operating System begins to boot. If the VIP stops booting with a “kernel panic” error, follow steps 20 through 24 to recover. Otherwise, skip to step 25.

20. Place the **VIP OS Restore #1 CD** in the VIP CD tray. Power down and power up the VIP.

NOTE: 2. Be prepared to **quickly** enter the next command at the *boot:* prompt.

21. Type **expert** and press **<Enter>**. The rescue image begins booting and will stop with the following message:

    *Please specify an alternate tape device, or hit **<Enter>** to boot from the CD/ floppies*

22. Press **<Enter>** again. The CD will finish booting. The VIP displays a black text screen with the following message:

    Please wait
    sh: can't access tty; job control turned off
    #

23. At the pound sign (#) prompt, type **post-nuke** and press **<Enter>**. The procedure will take about 2 seconds to run. When completed, the script will report that the post-nuke finished after displaying the partition table information.

24. Press the CD eject button to open the CD tray. Remove the CD. Press **<Ctrl-Alt-Del>** together to reboot the VIP.

NOTE: 3. If the *Welcome to Kudzu* screen appears, be prepared to quickly press the space bar.

25. The Red Hat Linux 7.3 Operating System will continue to boot. Prior to the login screen, a blue screen with a *Welcome to Kudzu* message may display. This is a timed screen, so do not delay. Immediately **press the space bar** to proceed. Both, one, or neither of the following two scenarios described in steps 26 and 27 may occur.

26. The *Hardware Removed* screen may display with the text *The following video adapter has been removed...*. If this screen is not displayed, skip to step 27. Otherwise, remove the hardware by using the left and right arrow keys to select the *Remove Configuration* button and press **<Enter>***.* A *Hardware Added* screen for the nVidia Video Adapter may display. If not, proceed to the next step. Otherwise, configure the video card by using the left and right arrow keys to select the *Configure* button and press **<Enter>**.

27. The *Hardware Removed/Changed* screen may display with the text *The mouse has changed*. If this screen is not displayed, skip to step 28. Otherwise, keep the current configuration by using the left and right arrow keys to select the *Keep current configuration* button and press **<Enter>***.*

28. The system will continue booting. If a GUI Linux login screen appears, skip to step 31. If a GUI Linux login screen does not appear and instead a text login prompt appears, continue with steps 29 and 30 to reboot the system and try again.

29. At the login prompt, type **root** and enter the root password **nws2004** when prompted.

30. Type **/sbin/shutdown -r now** to shutdown the VIP and reboot. The system will continue booting, and a GUI Linux login screen appears.

NOTE: 4. Steps 31 through 42 will configure the VIP network address.

31. At the VIP login screen, type **root** and press **<Enter>**.
32. Type the root password **nws2004** and press **<Enter>**.
33. Click the **KDE Gear** icon in the lower left corner of the screen.
34. Click **System**.
35. Click **Network Configuration**.
36. In the *Network Configurator* window, click **Active eth0 device**.
37. Click **Edit.** Change the IP address and default Gateway value to match the VIP entry in the 0MP `/etc/hosts` file. For example, the entry at the NWSHQ Test Bed site is 165.92.20.121. Ensure the Netmask is **255.255.0.0**.
38. Click **OK**.
39. Click **Apply**.
40. Click **Deactivate**.
41. Click **Activate**.
42. Click **Close**.

NOTE: 5. Steps 43 through 57 will configure the site-specific IP addresses in the VIP hosts file and change VIP passwords.

43. Click the **KDE Gear** icon in the lower left area of the screen.
44. Click **Editors**.
45. Click **KEDit**.
46. Click **File**.
47. Click **Open**.
48. In the *Location* box, type **/etc/hosts**.
49. Click **OK**. If there is a duplicate set of IP addresses, delete the second set.
50. Change the **entries** to match those for **VIP**, **0MP**, **5MP**, **as1**, and **as2** in the 0MP `/etc/hosts` file. For example, the 0MP entry at the NWSHQ Test Bed site is 165.92.20.111. Also, change the entry for **as1f** so it is consistent with the site's subnet.

51. Click **File** and select **Save**.
52. Click **File** and select **Quit**.
53. Click the **Shell** icon (lower left area of the screen) to open a *Shell* window.
54. To verify the `/etc/hosts` file, type **`ping 0MP`** and press **<Enter>**; then type **`ping 5MP`** and press **<Enter>**. Press **<Ctrl-C>** to exit the command.

NOTE: 6. If you do **not** need to configure the remote SFTP function, skip step 55.

55. Type **`chmod 666/etc/hosts`** and press **<Enter>** to allow configuration of the VIP for remote audio SFTP transmission.

NOTE: 7. Observe the following rules when defining good passwords:

a. A minimum of eight non-blank characters.
b. A minimum of one lowercase alphabetic character in the first eight characters.
c. A minimum of one uppercase alphabetic character in the first eight characters.
d. A minimum of one number in the first eight characters.
e. Six of the characters may occur only once in the password.
f. Password must be changed at least every 90 days.
g. Password must not be used in the last 11 password changes.
h. Password cannot contain default passwords or words in dictionary.
i. No special characters are allowed.

CAUTION

Do not use special characters in any of the CRS user account passwords. Even though the Department of Commerce password management policy specifies the use of at least one number or special character in the password, the CRS application software currently will not allow the use of special characters. The use of a special character in any password may cause the GUI login attempt to fail. Furthermore, the use of a special character in the root password may prevent access to the system. If this occurs, sites should consult Section A-7 (Lost Root User Password Recovery) of Appendix A (CRS Password Modification Procedures & Lost Root User Password Recovery) of the draft CRS System Administration Manual.

56. Create a crs user password by following the rules described in Note 7:
    a. Type **`su - crs`**, press **<Enter>**, then enter the crs password **nws2004** when prompted. If the command hangs and no prompt is returned, open a shell terminal by clicking on the Konsole icon (fourth from the lower left in the display) and entering the commands in steps b and c. Otherwise skip to step d.
    b. Type **`killall stty -s 9`**, then press **<Enter>** to allow the command in step a to complete successfully.
    c. Type **`exit`**, then press **<Enter>** to close the shell terminal.
    d. Type **`passwd`**, then press **<Enter>** and follow the instructions to enter the same crs user password used for 0MP.
    e. Type **`exit`**, then press **<Enter>** to exit the crs user.
57. Create a root user password by following the rules described above in Note 7: Type **`passwd root`** and follow the instructions to enter the same root password used for 0MP.
58. End the login session by clicking the **KDE Gear** icon in the lower left area of the screen.
59. Click **Logout**. The *End Session* for root window appears.
60. Click **OK** and the *VIP Login* window is displayed.

4.2 Setting Up Installation and Site Information, CRS Network Information, Voice Settings, and Audio FTP Configuration

NOTE: 1. Use the *VIP Setup Wizard* to enter installation and site information, CRS network information, voice settings, and if necessary, audio SFTP configuration.

1. From the VIP *Login* window, log in as **crs** with the password set in step 56 of section 4.1. Double-click the **Voice Improvement Processor Application** icon on the desktop. The *VIPv3.1 Setup Wizard Welcome* window displays.

NOTE: 2. The *Setup Wizard* will only appear the first time the user logs in with the crs user password. Once the information in the Setup Wizard is entered, double-clicking on the VIP Application icon will result in the display of the main *VIP* menu. This information may be edited using the *Systems Settings* window available from the main *VIP* menu.

2. Click **Next**. The *VIPv3.1 Setup Wizard: Step 1* window displays.

NOTE: 3. Parts of the VIP system contain licensed software. You must read and accept the Speechify licensing agreement. Since not all sites will use the .mp3 ftp capability, acquisition of this license is the responsibility of the site. Information is provided in the agreement about the acquisition of this optional and inexpensive license. **All sites must accept the Speechify licensing agreement to continue with the setup.**

3. Click the box next to the statement: “I understand the above disclaimer.” and click **Next**. The *VIPv3.1 Setup Wizard: Step 2* window displays. Click **Next**.
4. Enter the installer’s name in the *Name of installer* box.
5. Select your site name from the scrollable list of sites.

NOTE: 4. Only 13 of 122 operational sites are licensed to use the Spanish Male (Javier) VIP voice. The VIP software will not allow any other sites to use the Spanish VIP voice. The following are Spanish VIP sites:

LOX - Los Angeles, CA	LWX - Washington, D.C.	EWX - Austin, TX
MTR - Monterey, CA	MFL - Miami, FL	BRO - Brownsville, TX
STO - Sacramento, CA	PDT - Pendleton, OR	EPZ- El Paso, TX
SGX - San Diego, CA	CAE - Columbia, SC	SJU - San Juan, PR
HNX - San Joaquin, CA		

Sites that are not in the above list shall not use the VIP Spanish voice.

6. Click **Next**. The *VIPv3.1 Setup Wizard: Step 3* window displays.
7. Enter the IP addresses for both the CRS 0MP and 5MP. For the CRS user “crs” password box, enter **TEST**. With the change to SFTP file transfers between the Master MP, this password is no longer used and is just a dummy. However, it cannot be left blank.
8. If you intend to use the VIP audio SFTP function, you must also enter the Gateway IP address. This step is optional.
9. Click **Next**. The *VIPv3.1 Setup Wizard: Step 4* window displays. This window allows you to set the rate and volume of the Tom voice.
10. Use the **slider bar** to adjust the default 0 rate and volume of the Tom voice. To assist you in setting these values, two buttons are available to play and stop playing text in the window.
11. Click **Next**. The *VIPv3.1 Setup Wizard: Step 5* window displays. This window allows you to set the rate and volume of the Donna voice.
12. Use the slider bar to adjust the default 0 rate and volume of the Donna voice. To assist you in setting these values, two buttons are available to play and stop playing text in the window.

NOTE: 5. The *VIPv3.1 Setup Wizard: Step 6* window will only display for the Spanish VIP sites listed in the Note 4 box following step 5. All other sites should skip steps 13 and 14 below.

13. Click **Next**. The *VIPv3.1 Setup Wizard: Step 6* window displays. This window allows you to set the rate and volume of the Javier voice.
14. Use the **slider bar** to adjust the default 0 rate and volume of the Javier voice. To assist you in setting these values, two buttons are available to play and stop playing text in the window.

15. Click **Next**. The *VIPv3.1 Setup Wizard: Step 7* window displays. This window allows you to optionally configure the VIP for remote audio SFTP transmission.

NOTE: 6. Remote SFTP may be used to populate Web servers by providing audio for every message processed by VIP. Audio uploads are either 16 kHz, 16-bit multimedia wav files or mp3 files. This is not a standard CRS function; if you wish to use this feature, it is strongly recommended that you first contact the regional AWIPS focal point for approval. Otherwise, skip step 16.

16. Enter the ***user***, ***password***, ***IP address***, and ***upload directory*** information for .wav file or .mp3 file. Then select **ON** to activate this function.
17. Click **Next**. The *VIPv3.1 Setup Wizard: Finished* window displays.
18. You have completed the VIP setup. Click **Finish**.
19. The main *VIP* menu displays.

NOTE: 7. If you did **not** configure the remote SFTP function, skip steps 20 - 24.

20. Click the **Konsole** icon (fourth from the lower left in the display).
21. Type **`su - root`** and press **<Enter>.** When prompted, enter the root ***`password`*** and press **<Enter>**.
22. Type **`chmod 644 /etc/hosts`** and press **<Enter>** to change the permissions back.
23. Type **`exit`** and press **<Enter>** to exit the root user.
24. Type **`exit`** and press **<Enter>** to close the shell.

PART 5 - RECOVERY OF VIP PRE-PROCESSOR SUBSTITUTION AND LOCAL DICTIONARIES

5.1 Recovery of Substitution Dictionaries

1. Place the diskette labeled "**tom-sub.dic**" in the drive. From the main *VIP* menu, click **Pre-Processor**. This will display the *Pre-Processor "Substitution Dictionary" Manager*.
2. Click **Options**, which displays a *pull-down* menu. From the pull-down menu, click **English Male Substitution Dictionary <Tom>**.
3. Click **Options**, which displays a *pull-down* menu. From the pull-down menu, click **Restore Current Substitution Dictionary From Floppy Disk**.

4. A dialog box is displayed that asks:

   Retrieve the "Tom Substitution" dictionary from floppy disk?

   Click **Yes**.

5. If the transfer of the dictionary is successful, a dialog box will display the following message:

   File upload complete for "tom-sub.dic".

   Click **OK**.

6. Remove the **tom-sub.dic** diskette from the drive and store it in a safe place. Use this diskette whenever it is necessary to restore the English Male Substitution Dictionary.

7. Place the diskette labeled "**mara-sub.dic**" in the drive. Click **Options**, which displays a *pull-down* menu. From the pull-down menu, click **English Female Substitution Dictionary <Donna>**.

8. Click **Options**, which displays a *pull-down* menu. From the pull-down menu, click **Restore Current Substitution Dictionary From Floppy Disk**.

9. A dialog box is displayed that asks:

   Retrieve the "Donna Substitution" dictionary from floppy disk?

   Click **Yes**.

10. If the transfer of the dictionary is successful, a dialog box will display the following message:

    File upload complete for "mara-sub.dic".

    Click **OK**.

11. Remove the **mara-sub.dic** diskette from the drive and store it in a safe place. Use this diskette whenever it is necessary to restore the English Female Substitution Dictionary. If you do not have a Spanish license, skip to step 17.

12. Place the diskette labeled **javier-sub.dic** in the drive. Click **Options**, which displays a *pull-down* menu. From the pull-down menu, click **Spanish Male Substitution Dictionary <Javier>**.

13. Click **Options**, which displays a pull-down menu. From the pull-down menu, click **Restore Current Substitution Dictionary From Floppy Disk**.

14. A dialog box is displayed that asks:

    Retrieve the "Javier Substitution" dictionary from floppy disk?

    Click **Yes**.

15. If the transfer of the dictionary is successful, a dialog box will display the following message:

    File upload complete for "javier-sub.dic".

    Click **OK**.

16. Remove the **javier-sub.dic** diskette from the drive and store it in a safe place. Use this diskette whenever it is necessary to restore the Spanish Male Substitution Dictionary. Please note that the operator has no choice in the name of the backup file; it will always be *javier-sub.dic*.

17. Click the **black x** to exit from the *Pre-Processor "Substitution Dictionary" Manager* window.

5.2 Recovery of Local Dictionaries

1. Place the diskette labeled "**tom-root.dic**" in the drive. From the main *VIP* menu, click **Dict Manager**. This will display the *Local Dictionary Manager*.

2. Click **Options**, which displays a *pull-down* menu. From the pull-down menu, click **English Male Dictionary <Tom>**.

3. Click **Options**, which displays a *pull-down* menu. From the pull-down menu, click **Restore Current Dictionary From Floppy Disk**.

4. A dialog box is displayed that asks:

    Retrieve the "Tom" dictionary from floppy disk?

    Click **Yes**.

5. If the transfer of the dictionary is successful, a dialog box will display the following message:

    File upload complete for "tom-root.dic".

    Click **OK**.

6. Remove the **tom-root.dic** diskette from the drive and store it in a safe place. Use this diskette whenever it is necessary to restore the English Male Local Dictionary.

7. Place the diskette labeled "**mara-root.dic**" in the drive. Click **Options**, which displays a *pull-down* menu. From the pull-down menu, click **English Female Dictionary <Donna>**.

8. Click **Options**, which displays a *pull-down* menu. From the pull-down menu, click **Restore Current Dictionary From Floppy Disk**.

9. A dialog box is displayed that asks:

    Retrieve the "Donna" dictionary from floppy disk?

    Click **Yes**.

10. If the transfer of the dictionary is successful, a dialog box will display the following message:

    File upload complete for "mara-root.dic".

    Click **OK**.

11. Remove the **mara-root.dic** diskette from the drive and store it in a safe place. Use this diskette whenever it is necessary to restore the English Female Local Dictionary. If you do not have a Spanish license, skip to step 17.

12. Place the diskette labeled **javier-root.dic** in the drive. Click **Options**, which displays a *pull-down* menu. From the pull-down menu, click **Spanish Male Dictionary <Javier>**.

13. Click **Options**, which displays a *pull-down* menu. From the pull-down menu, click **Restore Current Dictionary From Floppy Disk**.

14. A dialog box is displayed that asks:

    Retrieve the "Javier" dictionary from floppy disk?

    Click **Yes**.

15. If the transfer of the dictionary is successful, a dialog box will display the following message:

    File upload complete for "javier-root.dic".

    Click **OK**.

16. Remove the **javier-sub.dic** diskette from the drive and store it in a safe place. Use this diskette whenever it is necessary to restore the Spanish Male Local Dictionary. Please note that the operator has no choice in the name of the backup file; it will always be *javier-sub.dic*.

17. Click the **black x** to exit from the *Local Dictionary Manager* window.

PART 6 - TERMINATION OF THE CRS BUILD 9.0.1 APPLICATION SOFTWARE

6.1 Validating and Verifying the CRS Database

NOTE:	Before beginning the procedure, verify that the operational database is not contaminated by stopping and restarting the CRS application.

1. On a blank part of the desktop, click and hold the left mouse button to pop up the *CRS Utilities* menu. Select **XCRS_SITE Utility**, and release the mouse button. The *XCRS_Site Configuration Developer* window displays.

2. Click **Stop CRS System**. The system displays:

   The CRS System will be STOPPED. Continue?

3. Click **OK**. Wait for the CRS application to stop. All status icons in the system status window indicate *Red Down*.

4. To start the *CRS Build 9.0.1 Application* from the *XCRS_Site Configuration Developer* window, click **Start CRS System**. The system displays:

   The CRS System will be STARTED. Continue?

5. Click **OK**. Wait until the *watch* icon disappears to indicate that CRS is initiating. Then close the *XCRS_Site Configuration Developer* window by clicking **Exit**.

6. Verify that the system is operational by checking the *System Status* window. If the system does not start properly, the database needs to be restored by either installing a previous backup (*Database Backup/Recovery Window*) or reloading the *daily.ASC* ASCII database file from the *XCRS_Site Configuration Developer*. Once the system starts properly, proceed with the next step.

6.2 Terminating the CRS Application

1. On a blank part of the desktop, click and hold the left mouse button to pop up the *CRS Utilities* menu. Select XCRS_SITE Utility, and release the mouse button. The *XCRS_SITE Configuration Developer* window displays.

2. Click the **Stop CRS System**. The system displays:

   The CRS system will be STOPPED. Continue?

3. Click **OK**. Wait for the CRS application to stop. All status icons in the *System Status* window indicate *RED Down*. Click **Exit** to close the *XCRS_SITE Site Configuration Developer* window.

PART 7 - INSTALLATION AND VERIFICATION OF CRS BUILD 10.0 APPLICATION SOFTWARE AND MODIFICATION TO MAN MACHINE INTERFACE (MMI) TO REMOVE UNWANTED MESSAGES

7.1 Installing CRS Software Build 10.0 From the CD-ROM

1. On the *Main CRS* menu, click **System** to access the *System* pull-down menu.

2. Click **Exit to UNIX** in the *System* pull-down menu. The *Wish to exit CRS Control Interface?* window displays. Click **OK** to exit the Control Interface.

3. CRS displays the *Security Screen* on top of the login window. Click **Acknowledge** to continue the login process.

4. At the *Login GUI* window, log in as the **root** user. Click the **KDE Desktop Application Starter** (the big **K Wheel** icon) in the lower left section of the *KDE Desktop* panel.
5. Click **SCO Control Center** on the pop-up menu.

NOTE: 1. You may also start the *SCO Control Center* by clicking the **SCO Admin** (Swiss Army Knife) icon on the *KDE Desktop* panel.

6. Double-click **Software_Management**.
7. Double-click **Applications Installer**.
8. Insert the CRS Build 10.0 CD-ROM into the CD drive of the selected installation MP, then select **CD-ROM_1** from the *Install from:* prompt in the upper half of the *Application Installer* window. If the files are not automatically read, click **Update View**.
9. After the CRS application package icons (***crsopsais***, ***crsopsfpm*** and ***crsopsmpm***) are displayed immediately below the *Install from:* prompt, select **crsopsais**, and click **Install**.

NOTE: 2. ***crsopsfpm*** and ***crsopsmpm*** can only be installed indirectly through ***crsopsais***.

10. Respond to the prompts displayed in Part 7.2, “Responding to Installation Prompts.”

NOTE: 3. The *Add Application: crsopsais* window and the *auto-install* window display the installation activity log and prompts for the installation operator. The log information and the prompt sequences will vary depending on the responses to the prompts.

4. In some instances, the installation process may erroneously come to a halt following the completion of the installation on 0MP. If you receive no further messages, the software was not installed on 5MP or any of the FEPs. If this occurs, terminate the installation, shut down 0MP, and repeat section 7.1.

7.2 Responding to Installation Prompts

The installation prompts that follow assume a typical configuration (0MP, 5MP, 1FEP, and 4BKUP).

The prompt sequence begins with *prompt p1*. Unless otherwise indicated, prompts occur in sequence (*p1* ... *p11*).

p1 *Build [version] installation options* (default: a)

- ***a*** *all processors (0MP 5MP 1FEP 4BKUP | 5MP 0MP 1FEP 4BKUP)*
- ***f*** *front-end processors (1FEP 4BKUP)*
- ***m*** *MPs (0MP 5MP | 5MP 0MP)*
- ***s*** *specific processor*
- ***x*** *exit*

Select the installation default (option ***a***) to load the software on all processors. Press **<Enter>** to select the installation option.

If it is determined that the IP addresses in `/etc/inet/hosts` (preinstalled by the CRS software contractor at the factory) are not correct, then prompt *p2* displays.

p2 *Enter your CRS site ID (e.g., DLH or NRC1):*

Enter the correct local site ID. Entry of a valid site ID results in a comparison of a set of expected IP addresses and the actual IP addresses in `/etc/inet/hosts` on all accessible (online) CRS processors. Differences between expected and actual IP addresses are displayed and logged. The entry of an invalid site ID results in the display of prompt *p2* again. If only the **<Enter>** key is pressed, the *p3* prompt will be displayed. Otherwise, the *p4* prompt will be displayed.

p3 *Clean out (reset) log files? (default: y)*

An affirmative response (y) to this prompt results in the display of a list of all valid CRS site IDs and their associated site locations (city, state, region). The list is presented in “pages” via the UNIX utility “pg”. Press **<Enter>** or **<+>** to display the next page, press **<->** to display the previous page, and press **<q>** to redisplay prompt *p2*. A negative response (n) results in the redisplay of prompt *p2*.

p4 *Clean out (reset) log files? (default: y)*

An affirmative response (y) to this prompt results in the resetting of all the CRS application software log files on all the processors in the configuration. A negative response (n) results in no changes to the CRS log files on any of the processors. It is normally good practice to clean the log files when a new software release is installed.

p5 *Change CRS system date and time? (default: n)*

An affirmative response (y) to this prompt results in a sequence of additional prompts beginning with *p6*. The entered date will be used to change the date and time on all the processors. A negative response (n) results in no changes to the current system date and time (displayed prior to the prompt); the next prompt will be *p11*.

p6 *Enter year (e.g., 1997):*

p7 *Enter month (e.g., 01<=mm<=12):*

p8 *Enter day (e.g., 01<=dd<=31):*

p9 *Enter hour (e.g., 00<=HH<23):*

p10 *Enter minute (e.g., 00=MM<=59):*

p11 Build [version] will be installed on the following processors:

[0MP | 5MP | 1FEP | 4BKUP ...]

with the following options:

Detected configuration is typical

[0MP / 5MP] remains CRS master (and X-window client) [0MP / 5MP] remains CRS shadow (and X-window server)

[Log files will be cleaned (reset on [5MP 0MP 1FEP 4BKUP]

Proceed with Build [version] installation? (default: y)

An affirmative response (y) to this prompt results in the installation of the CRS application software with the appropriate constraints indicated. A negative (n) response results in the display of a *Message* dialog window with the text: *User does not have permission to install packages pkgadd*. Clicking **OK** terminates the installation.

The master and shadow states that exist on the MPs at the time of installation should be preserved, if possible. Otherwise, the installation scripts determine new MP states, based on the old MP states, whether software is being installed on them and/or they are online.

The installation process will take approximately 15 to 20 minutes.

7.3 Post-Installation Caveats and Conventions

NOTE:

1. Software is installed on CRS processors in a predefined sequence (MPs, then FEPs). When the software has been successfully installed on a processor other than the installation MP, that processor is automatically shut down (and restarted). Because the FEPs share a single console (monitor and keyboard), only one of the FEPs—the one to which the console is physically connected through the switch box—starts itself automatically, following the shutdown. The startup sequence on an FEP that is not connected to a keyboard pauses while waiting for an **<F1>** key to be pressed at the keyboard. To complete the startup sequence for an FEP that is "stuck" waiting for the **<F1>** key to be pressed, connect (via the switch box) the keyboard to the FEP, verify that it is waiting (prompt message on the monitor), and press the **<F1>** key.

   The FEP startup sequence problem may be resolved by performing the procedure in Appendix B of the CRS Maintenance Manual.

   While the installation is in progress, many messages are displayed in the *auto-install log* window on the console.

NOTE: 1. Continued

Messages are of three types: ERROR, INFO and WARNING. Most of these messages are also written to the installation log file (`/crs/install.log`)

All error and warning messages from the installation log file are displayed in the *auto-install log* window at the completion of installation, in the following format:

Installation ERRORS
[ERROR messages from the installation log file | None]
[Refer to the installation procedures for further assistance]
Installation WARNING
[WARNING messages from the installation log file | None]

Refer to section 7.4 for further assistance

2. Inspection of the `/crs/install.log` file, after installation of the CRS Build 10.0 software, may result in the following message:

`UX:lpadmin: WARNING: "/dev/term/a02s" is accessible by others`

This warning can be ignored.

1. Press **<Enter>** to continue. The system displays the following:

Continue [0MP | 5MP] shutdown? (Default: y)

NOTE: 3. Shutting down the installation MP [0MP | 5MP] is an option. It is not necessary to shut down after the software has been installed on an FEP. A shut down is RECOMMENDED after CRS software has been installed on an MP to ensure that the installation MP [0MP | 5MP] and the other MP [0MP | 5MP] are functionally synchronized as CRS master and CRS shadow.

2. Press **<Enter>**.

NOTE: 4. If valid errors and warnings are displayed, error and warning messages must be resolved before attempting to start the system.

If there are no error or warning messages (i.e., the installation log displays "None"), the reference to the installation procedures (see Note 1 above) is not displayed. The *auto-install log* window displays until the operator responds to the prompt noted in step 1.

An affirmative response (y or Enter) results in the automatic shutdown and restart of the installation MP. **Remove the CD when the procedure is completed.**

A negative response (n) results in the disappearance of the prompt and the auto-*install log* window unless the state (master or shadow) of the installation MP has been changed, in which case the prompt *Shutting down to synchronize MP functionality* informs the operator that the installation MP will be shutdown. (Shutdown occurs when the operator presses any key.)

7.4 Viewing the Installation Log File

Results of the installation are logged into the *auto-install* window and into a log file (/crs/install.log). Logged messages are of three types: ERROR, INFO, and WARNING. INFO messages can be ignored. ERROR and WARNING messages are summarized in the *auto-install* window at the completion of the installation. They must be resolved before the system is started.

All logged messages have the following format:

```
date: script: type: [...] on PROC
```

where:

`date` = `DDD MMM dd hh:mm:ss LLL YYYY`

- `DDD` day of week abbreviation (e.g., Thu = Thursday)
- `MMM` month of year abbreviation (e.g., Sep=September
- `dd` numeric day of month (e.g., 1<dd<31)
- `hh` hour of the day in military format (e.g., 00<hh<23)
- `mm` minute of the hour (e.g., 00<mm<59)
- `ss` second of the minute (e.g., 00<ss<59)
- `LLL` local standard time (e.g., PDT = Pacific Daylight Time)
- `YYYY` calendar year

`script` = name of shell script in which message is generated

`type` = ERROR | INFO | WARNING

`[...]` = ext describing a condition of the type indicated

PROC = processor (e.g., 0MP, 5MP, 3FEP, 4BKUP) on which condition described by the text occurred

7.5 Modification of MMI To Remove Unwanted Messages

1. If not already logged into CRS as **admin**, do so now.
2. On OMP, open a *UNIX Shell* window from the *Maintenance* menu.
3. Log in as the *root* user:

   `0MP{admin}` **`su -`** then press **<Enter>**

   Enter the root password, then press **<Enter>**.
4. Enter the following command to display the *SCOADMIN License Manager* window:

   `scoadmin license` then press **<Enter>**
5. The following three licenses will be displayed:

   * *Merge 4 Desktop Edition* (highlighted in black)
   SCO Advanced File and Print Server
   Unixware 7 Business Edition

   The first two licenses are DEMO licenses and are unregistered. They need to be removed.
6. Press **<Tab>** once to select **Host** on the top line.
7. Press the right arrow key to move the cursor to **License**, then press **<Enter>** to display the *License* pull-down menu.
8. Press the down arrow key to select **Remove** and press **<Enter>**.
9. A confirmation message will be displayed. Press the left arrow key to select **OK** and press **<Enter>**.
10. The remaining two licenses will be displayed. Repeat steps 5 through 8 to remove the SCO Advanced File and Print Server license.
11. Press **<Tab>** once to select **Host** on the top line and press **<Enter>**.
12. Press the down arrow key to select **Exit** and press **<Enter>** to exit the *SCOADMIN License Manager* window.
13. Type **`exit`**, then press **<Enter>** to exit root user.

PART 8 - CHANGING OF MP, FEP, AND LAN SERVER PASSWORDS

These procedures detail which CRS user account passwords will be changed and how to change them. The 0MP user terminal displays the *Login GUI* window. Log in as **admin**. The main *CRS GUI* window displays, followed by the *System Not Operational* dialog box. Click **OK**.

NOTE:

1. The following CRS user accounts are present on all CRS nodes: **root**, **crs**, **admin**, **maint** and **oper**.
2. The **switchmp** user account is only required on the 0MP and 5MP nodes. The **sysadm** user account is only required on the FEP nodes.
3. When changing system passwords, make sure the changes are made on each system node, i.e., 0MP, 5MP, 1FEP, 4BKUP and any remaining FEP nodes. Additionally, the LAN Server **root** user password must be changed.
4. The LAN server (ps8) root password is limited to a maximum of 8 characters. Therefore, if sites choose to have their root passwords match on all processors, they must limit them to 8 characters.
5. Please observe the following rules when defining good passwords:
   a. A minimum of eight non-blank characters.
   b. A minimum of one lowercase alphabetic character in the first eight characters.
   c. A minimum of one uppercase alphabetic character in the first eight characters.
   d. A minimum of one number in the first eight characters.
   e. Six of the characters may occur only once in the password.
   f. Password must be changed at least every 90 days.
   g. Password must not be used in the last 11 password changes.
   h. Password cannot contain default passwords or words in dictionary.
   i. No special characters are allowed.

CAUTION

Do not use special characters in any of the CRS user account passwords. Even though the Department of Commerce password management policy specifies the use of at least one number or special character in the password, the CRS application software currently will not allow the use of special characters. The use of a special character in any password may cause the GUI login attempt to fail. Furthermore, the use of a special character in the root password may prevent access to the system. If this occurs, sites should consult Section A-7 (Lost Root User Password Recovery) of Appendix A (CRS Password Modification Procedures & Lost Root User Password Recovery) of the draft CRS System Administration Manual.

8.1 Procedure for Changing Passwords on the MPs and FEPs

1. If you are not already logged into CRS as **admin**, do so now.
2. If a *UNIX Shell* window is not already open, open one from the *Maintenance* menu.
3. Log in as the *root* user:

   `0MP{admin}` **`su`** then press **<Enter>**

   Enter the root password, then press **<Enter>**.
4. Use the UNIX *passwd* command to change the user passwords on the 0MP node. For the exact syntax and usage of the command, use the *man passwd* command string.

   # **`passwd root`** then press **<Enter>**

   Follow the prompts to change the password.

NOTE: 1. User switchmp password change cannot use the **passwd** command from the switchmp user. If this is done, it will force CRS to do an MP switch. The switchmp password must be changed using the **passwd switchmp** command from root user.

`passwd switchmp` then press **<Enter>**

Follow the prompts to change the password.

`su - crs` and enter the crs password if prompted.
`0MP{crs}` **`passwd`** then press **<Enter>**

Follow the prompts to change the password.

`0MP{crs}` **`exit`** then press **<Enter>**
`su - admin`, press **<Enter>,** then enter the admin password if prompted.
`0MP{admin}` **`passwd`** then press **<Enter>**

Follow the prompts to change the password.

`0MP{admin}` **`exit`** then press **<Enter>**
`su - maint`, press **<Enter>**, then enter the maint password if prompted.
`0MP{maint}` **`passwd`** then press **<Enter>**

Follow the prompts to change the password.

`0MP{maint}` **`exit`** then press **<Enter>**
`su - oper`, press **<Enter>**, then enter the oper password if prompted.
`0MP{oper}` **`passwd`** then press **<Enter>**

Follow the prompts to change the password.

`0MP{oper}` **`exit`** then press **<Enter>**

5. Save the password warning and expiration information for all users except *root*. The following two commands must be entered for the following users: *crs*, *admin*, *maint*, *oper*, and *switchmp*

   # **`passwd -n 0 -w 14 -x 91 <user>`** then press **<Enter>**
   where <***user***> is *crs, admin, maint,* etc.

   # **`passwd -s <user>`**

   The output from the above command will display as follows:

   <user> <status> <today's date> 0 91 14

6. Exit the *root* user.

   # **`exit`** then press **<Enter>**

7. Log into the 5MP node using the *rsh* command:

   `0MP{admin}` **`rsh 5MP`** then press **<Enter>**

   Log in as the *root* user:

   `5MP{admin}` **`su`** then press **<Enter>**

   Enter the *root* password, then press **<Enter>**.

8. Use the UNIX `passwd` command to change the user passwords on the 5MP node. For the exact syntax and usage of the command, use the `man passwd` command string.

NOTE: 2. The passwords should be changed to match the 0MP node passwords.

`passwd root` then press **<Enter>**

Follow the prompts to change the password.

NOTE: 3. User switchmp password change cannot use the **passwd** command from the switchmp user. If this is done, it will force CRS to do an MP switch. The switchmp password must be changed using the **passwd switchmp** command from root user.

`# passwd switchmp` then press **<Enter>**

Follow the prompts to change the password.

`su - crs`, press **<Enter>**, then enter the crs password if prompted.
`5MP{crs}` **`passwd`** then press **<Enter>**

Follow the prompts to change the password.

5MP{crs} **exit** then press **<Enter>**
su - admin, press **<Enter>**, then enter the admin password if prompted.
5MP{admin} **passwd** then press **<Enter>**

Follow the prompts to change the password.

5MP{admin} **exit** then press **<Enter>**
su - maint, press **<Enter>**, then enter the maint password if prompted.
5MP{maint} **passwd** then press **<Enter>**

Follow the prompts to change the password.

5MP{maint} **exit**, then press **<Enter>**
su - oper, press **<Enter>**, then enter the oper password if prompted.
5MP{oper} **passwd** then press **<Enter>**

Follow the prompts to change the password.

5MP{oper} **exit** then press **<Enter>**

9. Save the password warning and expiration information for all users except *root*. The following two commands must be entered for the following users: *crs*, *admin*, *maint*, *oper*, and *switchmp*

   # **passwd -n 0 -w 14 -x 91 <user>** then press **<Enter>**
   where <***user***> is *crs, admin, maint,* etc.
   # **passwd -s <user>** then press **<Enter>**

   The output from the above command will display as follows:

   <user> <status> <today's date> 0 91 14

10. Exit the *root* user and the 5MP node by typing **exit** twice:

    # **exit** then press **<Enter>**
    5MP{admin} exit then press **<Enter>**

11. Log into the 1FEP node using the *rsh* command:

    0MP{admin} **rsh 1FEP** then press **<Enter>**

    Log in as the *root* user:

    $ **su** then press **<Enter>**

    Enter the *root* password.

12. Use the UNIX *passwd* command to change the user passwords on the 1FEP node. For the exact syntax and usage of the command, use the *man passwd* command string.

NOTE: 4. The passwords should be changed to match the 0MP node passwords where they exist. The sysadm password, which only exists on the FEPs, should be the same on all FEPs.

1FEP{root} **passwd root** then press **<Enter>**

Follow the prompts to change the password.

NOTE: 5. You cannot switch remotely to the sysadm user because of terminal emulator problems. Therefore, the sysadm password must be changed using the **passwd sysadm** command from root user.

1FEP{root} **passwd sysadm** then press **<Enter>**

Follow the prompts to change the password.

1FEP{root} **su - crs**, press **<Enter>**, then enter the crs password if prompted.
$ **passwd** then press **<Enter>**

Follow the prompts to change the password.

$ **exit** then press **<Enter>**
1FEP{root} **su - admin**, press **<Enter>**, then enter the admin password if prompted.
$ **passwd** then press **<Enter>**

Follow the prompts to change the password.

$ **exit** then press **<Enter>**
1FEP{root} **su - maint**, press **<Enter>**, then enter the maint password if prompted.
$ **passwd** then press **<Enter>**

Follow the prompts to change the password.

$ **exit** then press **<Enter>**
1FEP{root} **su - oper**, press **<Enter>**, then enter the oper password if prompted.
$ **passwd** then press **<Enter>**

Follow the prompts to change the password.

$ **exit** then press **<Enter>**

13. Save the password warning and expiration information for all users except *root*. The following two commands must be entered for the following users: *crs*, *admin*, *maint*, *oper*, and *sysadm*

1FEP{root} **passwd -n 0 -w 14 -x 91 <user>** then press **<Enter>**
where <***user***> is *crs, admin, maint,* etc.

1FEP{root} **passwd -s <user>** then press **<Enter>**

The output from the above command will display as follows:

<user> <status> <today's date> 0 91 14

1FEP{root} **exit** then press **<Enter>** to exit the root password.

14. Exit the 1FEP node by typing *exit*.

    $ **exit** then press **<Enter>**

15. Log into the 4BKUP node using the *rsh* command:

    0MP{admin} **rsh 4BKUP** then press **<Enter>**

    Log in as the *root* user:

    $ **su** then press **<Enter>**

    Enter the *root* password.

16. Use the UNIX *passwd* command to change the user passwords on the 4BKUP node. For the exact syntax and usage of the command, use the *man passwd* command string.

NOTE: 6. The passwords should be changed to match the 0MP node passwords where they exist. The sysadm password, which only exists on the FEPs, should be the same on all FEPs.

4BKUP{root} **passwd root** then press **<Enter>**

Follow the prompts to change the password.

NOTE: 7. You cannot switch remotely to the sysadm user because of terminal emulator problems. Therefore, the sysadm password must be changed using the **passwd sysadm** command from root user.

4BKUP{root} **passwd sysadm** then press **<Enter>**

Follow the prompts to change the password.

4BKUP{root} **su - crs**, press **<Enter>**, then enter the crs password if prompted.
$ **passwd**

Follow the prompts to change the password.

$ **exit** then press **<Enter>**
4BKUP{root} **su - admin**, press **<Enter>**, then enter the admin password if prompted.
$ **passwd** then press **<Enter>**

Follow the prompts to change the password.

$ **exit** then press **<Enter>**
4BKUP{root} **su - maint**, press **<Enter>**, then enter the maint password if prompted.
$ **passwd** then press **<Enter>**

Follow the prompts to change the password.

$ **exit** then press **<Enter>**
BKUP{root} **su - oper**, press **<Enter>**, then enter the oper password if prompted.
$ **passwd** then press **<Enter>**

Follow the prompts to change the password.

$ **exit** then press **<Enter>**

17. Save the password warning and expiration information for all users except *root*. The following two commands must be entered for the following users: *crs*, *admin*, *maint*, *oper*, and *sysadm*

    4BKUP{root} **passwd -n 0 -w 14 -x 91 <user>** then press **<Enter>**
    where <***user***> is *crs, admin, maint,* etc.
    4BKUP{root} **passwd -s <user>** then press **<Enter>**

    The output from the above command will display as follows:

    <user> <status> <today's date> 0 91 14

    4BKUP{root} **exit** to exit the root password.

18. Exit the 4BKUP node by typing *exit*.

    $ **exit** then press **<Enter>**

NOTE:	8. Sites with more than two FEP nodes should change passwords on the remaining FEPs as applicable. See the following steps.

19. Log into the 2FEP node using the *rsh* command:

    0MP{admin} **rsh 2FEP** then press **<Enter>**

    Log in as the *root* user:

    $ **su** then press **<Enter>**

    Enter the *root* password.

20. Use the UNIX *passwd* command to change the user passwords on the 2FEP node. For the exact syntax and usage of the command, use the *man passwd* command string.

NOTE: 9. The passwords should be changed to match the 0MP node passwords where they exist. The sysadm password, which only exists on the FEPs, should be the same on all FEPs.

2FEP{root} **passwd root** then press **<Enter>**

Follow the prompts to change the password.

NOTE: 10. You cannot switch remotely to the sysadm user because of terminal emulator problems. Therefore, the sysadm password must be changed using the **passwd sysadm** command from root user.

2FEProot} **passwd sysadm** then press **<Enter>**

Follow the prompts to change the password.

2FEP{root} **su - crs**, press **<Enter>**, then enter the crs password if prompted.
$ **passwd** then press **<Enter>**

Follow the prompts to change the password.

$ **exit** then press **<Enter>**
2FEP{root} **su - admin**, press **<Enter>**, then enter the admin password if prompted.
$ **passwd** then press **<Enter>**

Follow the prompts to change the password.

$ **exit** then press **<Enter>**
2FEP{root} **su - maint**, press **<Enter>**, then enter the maint password if prompted.
$ **passwd** then press **<Enter>**

Follow the prompts to change the password.

$ **exit** then press **<Enter>**
2FEP{root} **su - oper**, then press **<Enter>**, then enter the oper password if prompted.
$ **passwd** then press **<Enter>**

Follow the prompts to change the password.

$ **exit** then press **<Enter>**

21. Save the password warning and expiration information for all users except *root*. The following two commands must be entered for the following users: *crs*, *admin*, *maint*, *oper*, and *sysadm*

2FEP{root} **passwd -n 0 -w 14 -x 91 <user>** then press **<Enter>**
where <***user***> is *crs, admin, maint,* etc.

2FEP{root} **passwd -s <user>** then press **<Enter>**

The output from the above command will display as follows:

<user> <status> <today's date> 0 91 14

2FEP{root} **exit** then press **<Enter>** to exit the root password.

22. Exit the 2FEP node by typing *exit*.

    $ **exit** then press **<Enter>**

23. Log into the 3FEP node using the *rsh* command:

    0MP{admin} **rsh 3FEP** then press **<Enter>**

    Log in as the *root* user:

    $ **su** then press **<Enter>**

    Enter the *root* password.

24. Use the UNIX *passwd* command to change the user passwords on the 3FEP node. For the exact syntax and usage of the command, use the *man passwd* command string.

NOTE: 11. The passwords should be changed to match the 0MP node passwords where they exist. The sysadm password, which only exists on the FEPs, should be the same on all FEPs.

3FEP{root} **passwd root** then press **<Enter>**

Follow the prompts to change the password.

NOTE: 12. You cannot switch remotely to the sysadm user because of terminal emulator problems. Therefore, the sysadm password must be changed using the **passwd sysadm** command from root user.

3FEP{root} **passwd sysadm** then press **<Enter>**

Follow the prompts to change the password.

3FEP{root} **su - crs**, press **<Enter>**, then enter the crs password if prompted.
$ **passwd** then press **<Enter>**

Follow the prompts to change the password.

$ **exit** then press **<Enter>**
3FEP{root} **su - admin**, press **<Enter>**, then enter the admin password if prompted.
$ **passwd** then press **<Enter>**

Follow the prompts to change the password.

$ **exit** then press **<Enter>**
3FEP{root} **su - maint**, press **<Enter>**, then enter the maint password if prompted.
$ **passwd** then press **<Enter>**

Follow the prompts to change the password.

$ **exit** then press **<Enter>**

3FEP{root} **su - oper**, press **<Enter>**, then enter the oper password if prompted.
$ **passwd** then press **<Enter>**

Follow the prompts to change the password.

$ **exit**

25. Save the password warning and expiration information for all users except *root*. The following two commands must be entered for the following users: *crs*, *admin*, *maint*, *oper*, and *sysadm*

3FEP{root} **passwd -n 0 -w 14 -x 91 <user>** then press **<Enter>**
where <***user***> is *crs, admin, maint,* etc.
3FEP{root} **passwd -s <user>** then press **<Enter>**

The output from the above command will display as follows:

<user> <status> <today's date> 0 91 14
3FEP{root} **exit**, then press **<Enter>** to exit the root password.

Exit the 3FEP node by typing *exit*.

$ **exit** then press **<Enter>**

26. Exit the *UNIX Shell* window by typing *exit*.

0MP{admin} **exit** then press **<Enter>**

8.2 Procedure for Changing the LAN Server (ps8) Password

NOTE: 1. The CRS and VIP application software should not be running. If the CRS application software is running, stop the CRS application by clicking the **System** menu, selecting **Stop System**, and then selecting **OK**. Wait until the application completely stops. If the VIP application is running, stop the VIP application by clicking **Stop** on the main VIP menu.

1. Open a *UNIX Shell* window from the *Maintenance* menu.
2. Type:

   `telnet ps8` then press **<Enter>**
3. Log in as *root* user and enter the *root* password (default password is **dbps**).
4. Type:

   `newpass` then press **<Enter>**
5. The system prompts:

   `Current password:` [enter current password] then press **<Enter>**
6. The system prompts:

   `new password:` [enter new password] then press **<Enter>**

NOTE: 2. No more than 8 characters are allowed in the password.

7. The system prompts:

   `repeat new password:` [re-enter new password] then press **<Enter>**
8. Type:

   `exit`, then press **<Enter>** to exit the LAN Server.

8.3 Procedure for Changing the CRS User Password in the /data/fxa/workFiles/nwr/nwr.cfg File on the AWIPS DS1 Node

AWIPS System Assumptions

The `/data/fxa/workFiles/nwr/nwr.cfg` has been correctly configured on the site DS1 node. The file should contain, in strict order, the following information: CRS user name, CRS user password, and the interface type **LAN**. The CRS user password must be changed to match that used in CRS. See the following example:

ds1-nmtw{awipsusr}2: cat /data/fxa/workfiles/nwr/nwr.cfg
crs
XXXXX [Verify the correct crs user password here]
LAN
ds1-nmtw{awipsusr}3:

NOTE: Based on your system configuration, change your CRS password on every AWIPS node where the *nwr.cfg* file exists. For example, if you run transferNWR on workstations to ftp messages to CRS, the CRS password must be changed there as well. If you are unsure of your specific configuration, please check with the AWIPS focal point.

8.4 Shut Down and Restart Both MPs

1. If a *UNIX Shell* window is not already open, open one from the *Maintenance* menu.
2. Type **`su -`** press **<Enter>**, then enter the root password to log in as the *root* user.
3. Type **`rsh 5MP /sbin/shutdown -y -i0 -g0`** then press **<Enter>** to begin the shutdown process on 5MP. 5MP will shut down, and the last message on the 5MP terminal will prompt the user to press any key to start the system.
4. Type **`cd/`** then press **<Enter>** to change to the root directory on 0MP.
5. Type **`/sbin/shutdown -y -i0 -g0`** then press **<Enter>** to begin the shutdown process on 0MP. 0MP will shut down, and the last message on the 0MP terminal will prompt the user to press any key to start the system.
6. Press **<Enter>** on the 0MP terminal to boot the 0MP. Repeat this on 5MP.
7. After a minute or so, both MPs will reboot completely and display the 0MP CRS login window. Log in to both terminals as **admin** then press **<Enter>**.

PART 9 - INSTALLATION OF SSH KEYS

NOTE:

1. This procedure requires a blank DOS formatted 1.44 MB diskette that will eventually contain the SSH Keys (after proceeding with the installation instructions) which will be referred to in this document as the keyfile diskette.
2. When the MPs and VIP are restarted following the installation of the CRS Build 10.0 and VIP 3.1, respectively, authentication key pairs (public and private) are installed. These keys will be used for sftp transactions between the MPs and VIP. **Because of loading concerns in AWIPS, it will not have the sftp capability. Transactions from AWIPS to CRS will continue to use ftp. However, Section C-6.1 of Appendix C of the draft System Administration Manual must be performed if and when AWIPS installs the sftp capability in order to update the public keys from AWIPS.**
3. The fixkey script is used in the following steps to copy keys to and from the keyfile diskette and the MPs and VIP. The steps that follow instruct the installer to open up UNIX shells on the VIP, 5MP, and 0MP respectively and start the fixkey script on all three processors. After each of the three processors have been set up to start copying the keys, the fixkey script will instruct the user to wait to make sure that the following five steps are performed in the proper order:

   #1. The diskette is placed in the 0MP diskette drive. If AWIPS public key files are present (and they will not), they are copied to 0MP. If they are present, there can be as many as nine. If they are not present (and they will not), the script displays a warning message to that effect. The 0MP host and crs user keys are copied to the diskette.

   #2. Step 1 is repeated for 5MP.

   #3. The diskette is placed in the VIP diskette drive. The 0MP and 5MP host and crs user keys are copied to the VIP. The VIP host and crs user keys are copied to the diskette. The VIP fingerprint report is copied to the diskette.

   #4. The diskette is placed in the 0MP diskette drive. The VIP host and crs user keys are copied to 0MP. The 0MP fingerprint report is copied to the diskette.

   #5. Step 4 is repeated for 5MP.

   Once the setup for the keyfiles is complete, the scripts can be started in the order described above.

NOTE: 4. The fingerprint report files shall be retained as a record of the authentication key generation. The keyfile diskette should be labeled, dated, and initialed. It should be stored in a secure manner in a locked container that is consistent with the DOC password hard copy storage requirements.

1. If you are not already logged in as **crs** on the VIP, do so now. Click the **Konsole** icon (fourth from the lower left in the display) to display a *UNIX Shell* window. Enter the following commands at the prompt:

2. Type:

   su -

   Press **<Enter>** and type in the appropriate root password.

3. Type:

   fixkeysv.sh

   Press **<Enter>**.

   This will start the fixkey script described in Note 3.

CAUTION

Do not press the <ENTER> key as requested by the displayed text message. Proceed to the next step.

The following message will be displayed on the screen:

Ready for Step #3 of fixkeysv.sh procedure running on system VIP.
This procedure sets up ssh configuration/key files in CRS/VIP.
If you did not want to run fixkeysv.sh use the CNTL-C key to exit.

First - did you complete Step #2 with the floppy on the 5mp computer?
At Step #3 place the keyfile diskette in the VIP floppy drive and press ENTER:

4. Simultaneously press the **<Ctrl-Ctrl>** keys. This will move the video display, mouse, and keyboard to the 5MP.

NOTE: 5. The operator will open two UNIX shells. One will be used to run the fixkey script on 0MP. The other one will remote shell to 5MP to run the fixkey script there.

5. On the *CRS Main* menu, click **Maintenance** and then click **UNIX Shell** to open a UNIX shell. Repeat this to open a second UNIX shell. Position the two shells so that one is in the top half of the window and the second is in the bottom half.

6. Click the bottom **UNIX Shell** and enter the following commands at the prompt:
7. Type:

   `rsh 5mp`

   Press **<Enter>**. This will remote shell to 5MP.

8. Type:

   `su -`

   Press **<Enter>** and enter the root password.

9. Type:

   `/etc/config/fixkeys.sh`

   Press **<Enter>**.

   This will start the fixkey script described in Note 3.

CAUTION

Do not press the <*ENTER*> key as requested by the displayed text message. Proceed ato the next step.

The following message will be displayed on the screen:

Ready for Step #2 of fixkeys.sh procedure running on system 5MP.
This procedure sets up ssh configuration/key files in CRS/VIP.
If you did not want to run fixkeys.sh use the DELETE key to exit.

First - did you complete Step #1 with the floppy on the 0mp computer?
At Step #2 place the keyfile diskette in the 5MP floppy drive and press ENTER:

10. Leave the *5MP* UNIX shell by clicking on the **UNIX Shell** in the top half of the window. This is the *0MP* window. Enter the following commands at the prompt:
11. Type:

    `su -`

    Press **<Enter>** and type in the appropriate root password.

12. Type:

    `/etc/config/fixkeys.sh`

    Press **<Enter>**.

This will start the fixkey script described in Note 3.

CAUTION

Do not press the <ENTER> key as requested by the displayed text message. Proceed to the next step.

The following message will be displayed on the screen:

Step #1 of fixkeys.sh procedure running on system 0MP.
This procedure sets up ssh configuration/key files in CRS/VIP.
If you did not want to run fixkeys.sh use the DELETE key to exit.

If you have AWIPS keyfiles they should already be on your dos format keyfile diskette. When you are ready for Step #I, place the keyfile diskette in the 0MP floppy drive and press ENTER:

NOTE: 6. All three processors are now set up to start the copying of the keys. The previous warnings not to press <Enter> allow for an orderly and proper installation. If there are any problems and/or operator errors in completing the following steps, the installation will abort.

13. Insert the **keyfile diskette** in the **0MP** diskette drive and press **<Enter>** to perform fixkey script (step 1). The following message will be displayed on the screen:

Step #1 in progress.

Deleting any awips.pub files not on the floppy already in /crs/.ssh.
WARNING: The AWIPS keyfile not found. You will have no AWIPS SFTP.
This is only proper if your AWIPS has not yet implemented ssh.
When AWIPS has ssh and a keyfile this procedure must be rerun.
At that time the files should be on the keyfile floppy as awips#.pub - for example awips1.pub. Multiple files each with a single public key are allowed - the floppy may have awips1.pub and awps2.pub.
Please see your CRS/VIP Software Installation Procedure for further information.

Remaining CRS/VIP key installation without AWIPS will proceed if you press ENTER. Otherwise use DELETE/CNTRL -C to stop fixkeys procedure on all boxes and start again with a corrected floppy.

NOTE: 7. Since AWIPS will not have the sftp capability when CRS Build 10.0/VIP 3.1 is implemented, do not be concerned with the warning described above. **It is important to note, however, that Section C-6.1 of Appendix C of the draft System Administration Manual must be performed when AWIPS adds the sftp capability.**

14. Press **<Enter>** to resume copying the keyfiles. The following message will be displayed on the screen:

    Step #1 completed - now move the keyfile diskette to the
    5mp computer floppy drive for Step #2.

    When ready for Step #4 after 5mp and vip steps,
    At Step #4 replace the keyfile diskette in the 0MP floppy drive and
    press ENTER:

15. Remove the **keyfile diskette** from the **0MP** diskette drive and insert it into the **5MP** diskette drive. Leave the 0MP UNIX shell by clicking on the **5MP Unix Shell**, and press **<Enter>** to perform script step 2. The following message will be displayed on the screen:

    Step #2 in progress.
    Deleting any awips.pub files not on the floppy already in /crs/.ssh.
    WARNING: The AWIPS keyfile not found. You will have no AWIPS SFTP.
    This is only proper if your AWIPS has not yet implemented ssh.
    When AWIPS has ssh and a keyfile this procedure must be rerun.
    At that time the files should be on the keyfile floppy as awips#.pub
    - for example awips1.pub. Multiple files each with a single public
    key are allowed - the floppy may have awips1.pub and awps2.pub.
    Please see your CRS/VIP Software Installation Procedure for further information.

    Remaining CRS/VIP key installation without AWIPS will proceed if you press ENTER. Otherwise use DELETE/CNTRL -C to stop fixkeys procedure on all boxes and start again with a corrected floppy.

NOTE: 8. Since AWIPS will not have the sftp capability when CRS Build 10.0/VIP 3.1 is implemented, do not be concerned with the warning described above. **It is important to note, however, that Section C-6.1 of Appendix C of the draft System Administration Manual must be performed when AWIPS adds the sftp capability.**

16. Press **<Enter>** to resume copying the keyfiles. The following message will be displayed on the screen:

    Step #2 completed - now move the keyfile diskette to
    the vip computer floppy drive for Step #3.

    When ready for Step #5 after the vip Step #3,
    At Step #5 replace the keyfile diskette in the 5MP floppy drive and press ENTER:

17. Remove the **keyfile diskette** from the **5MP** diskette drive and insert it into the **VIP** diskette drive. Simultaneously press the **<Ctrl-Ctrl>** keys to return the video display, mouse, and keyboard to the VIP and press **<Enter>** to perform fixkey script (step 3). The following message will be displayed on the screen:

    Step #3 in progress
    CRS VIP fixkeysv.sh - 0mp pub file found.
    CRS VIP fixkeysv.sh - 5mp pub file found.
    CRS VIP fixkeysv.sh - 0mphostrsa.pub file found.
    CRS VIP fixkeysv.sh - 5mphostrsa.pub file found.
    Fixing /home/crs/.ssh/authorized_keys for 0mp and 5mp.
    Fixing /etc/ssh/ssh_known_hosts with 0MP 5MP host info.
    0mp host rsa pub key: /home/crs/.ssh/fprnt.VIP
    5mp host rsa pub key: /home/crs/.ssh/fprnt.VIP
    Stopping sshd
    Starting sshd
    Step #3 complete. VIP ssh key configuration done.
    Remove floppy and take to 0mp for Step #4.
    End fixkeysv.sh script Step III done, fingerprint report in
    /home/crs/.ssh/fprnt.VIP.

18. Simultaneously press the **<Ctrl-Ctrl>** keys to return the video display, mouse, and keyboard to the MP.

19. Click the **0MP UNIX Shell** and move the **keyfile diskette** to the **0MP** diskette drive. Press **<Enter>** to perform script step 4. The following message displays on the screen:

    Step #4 in progress.
    CRS 0MP fixkeys.sh - vip.pub file found.
    CRS 0MP fiskeys.sh - viphostrsa.pub file found.
    Configuring AWIPS/CRS/VIP keydata on 0MP.
    Fixing /crs/.ssh/authorized_keys for awips and vip.
    UX:LS: ERROR: Cannot access /crs/.ssh/awips.pub: No such file or directory*
    Fixing /usr/local/etc/ssh_known_hosts with vip host info.
    0MP fingerprint report in /crs/.ssh/fprnt.0MP.
    After Step #4 on 0mp move floppy to 5mp for Step #5
    Step #4 complete. 0MP ssh key configuration done.

20. Click the **5MP UNIX Shell** and move the **keyfile diskette** to the **5MP** diskette drive. Press **<Enter>** to perform script step 5. The following message displays on the screen:

    Step #5 in progress.
    CRS 5MP fixkeys.sh - vip.pub file found.
    CRS 5MP fiskeys.sh - viphostrsa.pub file found.
    Configuring AWIPS/CRS/VIP keydata on 5MP.
    Fixing /crs/.ssh/authorized_keys for awips and vip.
    UX:LS: ERROR: Cannot access /crs/.ssh/awips.pub: No such file or directory*
    Fixing /usr/local/etc/ssh_known_hosts with vip host info.
    5MP fingerprint report in /crs/.ssh/fprnt.5MP.
    Last step.
    Step #5 complete. 5MP ssh key configuration done.

21. Verify that all the key files have been saved on the keyfile diskette by typing:

    `mdir a: >>temp.txt` then press **<Enter>**.

    Type: **`cat temp.txt`** then press **<Enter>**

    The following files should be displayed (with different date/time stamps):

```
Directory for A:/

0mp             pub     597    06-16-2004      9:04    0mp.pub
0MPHOS~1        PUB            06-16-2004      9:04    0mphostrsa.pub
stp1                           06-16-2004      9:04    stp1
vip             pub            06-16-2004      14:14   vip.pub
5mp             pub            06-16-2004      9:14    5mp.pub
5MPHOS~1        PUB            06-16-2004      9:14    5mphostrsa.pub
stp2                           06-16-2004      9:14    stp2
VIPHOS~1        PUB            06-16-2004      14:15   viphostrsa.pub
stp3                           06-16-2004      14:15   stp3
fprnt           VIP            06-16-2004      14:14   fprnt.VIP
fprnt           0MP            06-16-2004      9:19    fprnt.0MP
stp4                           06-16-2004      9:19    stp4
stp0                           06-16-2004      9:20    stp0
fprnt           5MP            06-16-2004      9:20    fprnt.5MP
stp5                           06-16-2004      9:20    stp5
```

22. **Remove the keyfile diskette and label it, date it, and initial it. Store it in a locked, safe place in accordance with the DOC password security policy.** Type the following commands to close the *5MP UNIX Shell*:

23. Type:

    `exit`

    and press **<Enter>** to exit root user.

24. Type:

    `exit`

    and press **<Enter>** to exit 5MP.

25. Type:

    `exit`

    and press **<Enter>** to close shell.

26. Click the **0MP UNIX Shell** and enter the following commands to close it:

27. Type:

    `exit`

    and press **<Enter>** to exit root user.

28. Type:

    `exit`

    and press **<Enter>** to close shell.

29. Simultaneously press the **<Ctrl-Ctrl>** keys to return the video display, mouse, and keyboard to the VIP. Enter the following commands to close the *VIP UNIX Shell*:

30. Type:

    `exit`

    and press **<Enter>** to exit root user.

31. Type:

    `exit`

    and press **<Enter>** to close shell.

NOTE: 9. * FOR USERS OF THE VIP REMOTE SFTP ONLY *****

All the VIP Remote FTP users must convert to a standard configuration supported by CRS B10/VIPB3.1. The VIP B3.1 requires sites to dump the VIP messages to the LDAD Server (LS1), and then either push them out to the external system or have the external system retrieve them from LS1. This section provides step-by-step instructions to accomplish this. However, it will be each site's responsibility to move the messages from LS1 to the external system.

Users of the VIP Remote SFTP (formerly Remote SFTP) capability must copy the **vip.pub** key on the keyfile diskette from the previous steps to the LS1.

The operator should coordinate this step with the LS1 System Administrator.

a. Create **crs** user account on the LS1.

b. Log on the LS1 as **crs** then press **<Enter>**.

c. Verify the `/home.crs/.ssh` directory exists with protection of *700*.

d. If the directory does not exist, create one with the following instructions:

`mkdir /home/crs/.ssh` then press **<Enter>**

`chmod 700 /home/crs/.ssh` then press **<Enter>**

e. Verify the *`authorized_keys`* file exists on `/home/crs/.ssh`.

f. If the *`authorized_keys`* file exists, remove it with the following instructions:

`rm /home/crs/.ssh/authorized_keys`

g. Create a new *`authorized_keys`* file by copying the **`vip.pub`** file from the keyfile diskette to **`/home/crs/.ssh/authorized_keys`** on LS1. No specific instructions for doing this are included; each site may determine the most appropriate manner to accomplish this task.

h. Create an entry for the LDAD server in the VIP routing table by doing the following at the VIP:

Click **KDE Gear**.

Click **System**.

Click **Network Configuration**.

Select **Active etho device**.

Click **Edit**.

Click **route** tab and click **add**. Fill out the *Address, Subnet Mask*, and *Gateway IP Address* boxes. The *Address* is the ***LS1 IP Address***. The *Subnet Mask* is **255.255.255.255**. The *Gateway IP Address* is the site's ***Gateway IP Address***.

Click **OK** twice; then click **Apply**, and **Close**.

i. Restart the network by doing the following at the VIP:

Click the **Konsole** icon (fourth from the lower left in the display).
Type **`su -`** , press **<Enter>**, and when prompted, enter the **`root`** password, then press **<Enter>**.
Type **`service network restart`**, then press **<Enter>**. The system will return several network interface messages.
Type **`exit`** then press **<Enter>** to exit the root user.

j. Additionally, the operator must approve the remote fingerprint of the target system by doing the following at the VIP:

Type **`sftp xxx.xxx.xxx.xxx`** then press **<Enter>**
where ***`xxx.xxx.xxx.xxx`*** is the LS1 IP address

The operator will be asked:

RSA key fingerprinting is xxxxxxx
Are you sure you want to continue connecting (yes/no)?

The operator should answer **yes**. This will add the LS1 host to the `known_hosts` file on the VIP.

Type **`quit`** then press **<Enter>**.

Type **`exit`** then press **<Enter>** to close the shell.

Logons and transfers into VIP from outside of CRS are not authorized to be added to the VIP computer. Likewise, outside generated public keys are **NOT** to be added to the VIP computer.

PART 10 - CRS AND VIP APPLICATION STARTUP AND VERIFICATION

10.1 Starting up the CRS Application

1. To start the CRS Build 10.0 Application, click the **System** menu and click **Start System**. The system displays the **Start CRS** dialog box, which prompts the user for a response.
2. Click **OK** to begin the startup sequence. The *CRS System is started* dialog box displays. Click **Close**.
3. If the *Status* window is not displayed, open it using the *System* pull-down menu. Click the **System Status** menu selection.
4. If the *Alert Monitor* window is not displayed, open it using the *System* pull-down menu. Click **Alert Monitor**.
5. In the *Status* window, verify the proper start of the CRS application. If the system does not start, notify the CRS Help Desk.
6. Verify the proper and normal operation of the system. The database has not changed, so all weather messages that were previously broadcasting will continue to broadcast, unless they have expired.

10.2 Starting Up the VIP Application

1. To run the VIP application, click **Start** on the main *VIP* menu.
2. At the *CRS Status* window on the CRS Master Console, verify that the *VIP* icon is a green arrow pointing up.

ATTACHMENT B
Sample EMRS Report